REMARKS/ARGUMENTS

In the final Office action dated September 14, 2005 all of the claims were rejected under 35 U.S.C. § 102. By this Amendment, Applicant has amended the specification, amended claims 1 - 4 and 6 - 9, canceled claim 6 and added claims 11 - 16. Reconsideration and reexamination are hereby requested for claims 1 - 5 and 7 - 16 that are now pending in this application.

Response to the 35 U.S.C. § 102 Rejection of the Claims

Claims 1 - 10 were rejected under 35 U.S.C. § 102 as being anticipated by Brown, et al., U.S. Patent No. 6,732,179 (hereafter "Brown"). Claims 1 and 7 are independent.

Brown is directed to a system that ensures that a user is authorized to access a service provided by a walled garden proxy server ("WGPS"). When a user wishes to access a service (via a client device 112) the client 112 must present a ticket to the WGPS via a network 412. Column 8, lines 1 - 2. The ticket contains user access bits that indicate which services the client is authorized to access. Column 11, lines 59 - 64. The user initiates access by authenticating himself/herself to a client device 112 (e.g., via a login password). The client 112 then sends a Box ID and user authentication information to a gateway server ("GS") via the network 412. Column 11, lines 50 - 56. After verifying the user authentication information, the GS generates a ticket and uses a key distributed by a keymaster to encrypt the entire ticket or the user access bits in the ticket. Column 12, lines 13 - 20.

The keymaster generates keys and sends the keys to the WGPS and other servers (e.g., the GS) in the system that are connected via network 412. To protect the keys, the keys are sent over the network via a secure SSL connection. To provide an added level of security, the keys are valid for a limited period of time. The keymaster periodically sends a new key to the server since eventually each key will expire. Column 10, lines 11 - 25.

The GS sends the encrypted ticket to the client 112 via the network 412. Since the client does not receive the key from the GS, the client cannot modify or decrypt the encrypted ticket. Column 12, lines 28 - 32. The client sends the encrypted ticket to the WGPS via the network 412 to request access to a service. Column 12, lines 39 - 43.

The WGPS uses the uses the key distributed by the keymaster to decrypt the entire ticket or the user access bits in the ticket. The WGPS then checks the user access bits to determine which services the user is authorized to access. Column 12, lines 43 - 55.

Claim 1

Claim 1 is directed to a "method for concealing a parameter transferred between a first and second device" comprising:

generating by the first device a control signal and a parameter signal;

encrypting or hashing by the first device a portion of the control signal with the parameter signal to generate an encrypted or hashed parameter signal and control signal;

transmitting by the first device to the second device the control signal and the encrypted or hashed parameter signal and control signal;

receiving by the second device from the first device the control signal and the encrypted or hashed parameter signal and control signal;

using the control signal to decrypt or inversely hash the encrypted or hashed parameter signal and control signal; and

generating by the second device a destination parameter signal depending upon a comparison of the control signal and the decrypted or inversely hashed control signal.

Initially, Applicant notes that the final Office did not state which elements of Brown read on which limitations of claim 1. Applicant assumes that the Examiner contends that either the client or the GS teaches the first device, the WGPS teaches the second device, and that the ticket teaches the control signal. However, neither combination of these components teaches or suggests claim 1.

The client 112 does not teach the first device because it does not generate "a control signal and a parameter signal" (e.g., it does not generate the ticket) and it does perform any encrypting or hashing. Rather, the GS generates the ticket and encrypts the ticket. Column 11, line 58 - 59 and column 12, lines 15 - 17.

The GS does not teach the first device because it does not

transmit "to the second device the control signal and the encrypted or hashed parameter signal and control signal." The GS sends the ticket to the client 112. Column 12, line 27 - 28. It is the client 112 that sends the ticket to the WGPS. Column 8, lines 1 - 2.

Moreover, the WGPS does not use "the control signal to decrypt or inversely hash the encrypted or hashed parameter signal and control signal." The WGPS does not receive an encrypted or hashed parameter signal and control signal. Rather, again assuming that the Examiner is contending that the ticket teaches the control signal, the WGPS only receives an encrypted ticket or portion of a ticket. Column 12, line 47 - 52.

Also, the WGPS does not receive "from the first device the control signal and the encrypted or hashed parameter signal and control signal." Brown states that the entire ticket may be encrypted and sent. Alternatively, Brown states that a portion (the access right bits 816) of the ticket may be sent, but does not state that this portion of the ticket is also sent in an unencrypted form at the same time. Hence, in this second scenario, the entire ticket is not sent in unencrypted form along with an encrypted portion.

Accordingly, Applicant submits that Brown does not teach or suggest all of the limitations of claim 1. Claims 2 - 5 and 11 that depend on claim 1 also are patentable over Brown the reasons set forth above. In addition, these dependent claims are patentable over the cited references for the additional limitations that these claims contain.

For example, claim 2 recites, in part: "generating by the first device a first key signal using the control signal." Neither the client 112 nor the GS generate any key signals. Rather, only the keymaster generates keys in Brown.

Claim 4 recites, in part: "generating by the first device a key index signal" and "generating by the first device a key variable signal." The client 112 and the GS do not generate any key signals such as these.

Claim 5 recites, in part: "generating by the second device the second key signal . . . using a hash function." The portion of Brown cited by the Examiner here (column 11, line 59 - column 12, line 12) merely lists the contents of the ticket. There is no mention of hashing here. Moreover, Applicant could not find any reference to the WGPS (assuming the Examiner contends the WGPS teaches the second device) or any other component of Brown using a hash function for any purpose.

Claim 11 recites, in part: "the control signal comprises a key index and the portion of the control signal comprises the key index." Brown does not teach or suggest encrypting or hashing a portion of a control signal comprising a key index.

Claim 7

Claim 7 is directed to an apparatus comprising:

> a control logic block to receive a control signal comprising a key index and an encrypted or hashed signal that comprises an encrypted or hashed form of a parameter signal and a portion of the control signal; and

an interface operation logic block operably coupled to the control logic block to decrypt or inversely hash the encrypted or hashed signal in accordance with the key index to generate a destination parameter signal.

Brown does not teach or suggest any component that receives "a control signal comprising a key index and an encrypted or hashed signal that comprises an encrypted or hashed form of a parameter signal and a portion of the control signal." The GS does not receive encrypted or hashed data. The client 112 and the WGPS only receive the encrypted ticket.

Accordingly, Applicant submits that Brown does not teach or suggest all of the limitations of claim 7. Claims 8 - 10 and 12 that depend on claim 7 also are patentable over Brown the reasons set forth above. In addition, these dependent claims are patentable over the cited references for the additional limitations that these claims contain.

For example, claim 9 recites, in part: "generate an intermediate key signal using a key index signal" and "generating a key signal using the intermediate key signal received from the key table module and a key variable signal." Brown does not generate three key separate signals as claimed.

Claim 12 recites, in part: "the portion of the control signal comprises the key index." Brown does not teach or suggest encrypting or hashing a key index.

New Claims

Applicant also has added claims 13 - 16. Claim 13 is independent. Claim 13 includes limitations such as "using, by the first device, at least a portion of the control signal to obtain a first cryptographic key" and "encrypting or hashing using the first cryptographic key, by the first device, a first signal to generate an encrypted or hashed signal." Claim 14 includes limitations such as "the second device stores the decrypted or inversely hashed parameter signal depending on a comparison of a portion of the control signal received from the first device and the decrypted or inversely hashed portion of the control signal." Claim 15 recites "the portion of the control signal comprises the key index." Claim 16 includes limitations such as "storing, by the second device, the decrypted or inversely hashed signal at a location determined in accordance with the destination register signal." Applicant submits that new claims 13 - 16 are not taught or suggested by Brown.

Finally, Applicant notes that in the Advisory Action the Examiner questioned the use of certain language in Applicant's response to the final action. Here, Applicant notes that it was not arguing that the claims recited "the entire ticket in unencrypted form and a portion of the ticket that is encrypted are both transmitted." Rather, since the final Office action had not pointed out which components of Brown read on particular elements of claim 1, Applicant thought it would be helpful to use the language of Brown (that Applicant assumed the Examiner

was referring to) to show how the teachings of Brown differ from the claims.

CONCLUSION

In view of the above amendments and remarks Applicant submits that the claims are patentably distinct over the cited references and that all the objections/rejections to the claims have been overcome. Reconsideration and reexamination of the above application is requested.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____

Stephen D. Burbach
Reg. No. 40,285
626/795-9900

SDB/sdb
VSJ PAS640114.1-*-08/25/05 5:13 PM